

UNITED STATES DISTRICT COURT

for the
District of Delaware

REDACTED

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)an Apple iPhone described in Attachment A located at
the FBI Office at 500 Delaware Avenue, Suite 300,
Wilmington, Delaware 19801

Case No.

21-207M

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the _____ District of _____ Delaware _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

FILED

The search is related to a violation of:

Code Section
18 U.S.C. 242

Deprivation of Civil Rights

Offense Description

SEP - 3 2021

The application is based on these facts:
See Affidavit Attached

U.S. DISTRICT COURT DISTRICT OF DELAWARE

☒ Continued on the attached sheet.☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

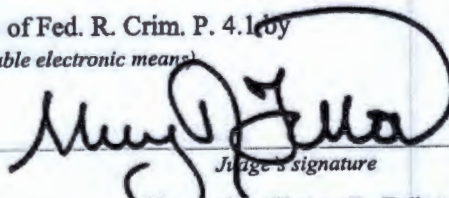
FBI Special Agent Joshua Wilson

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ (specify reliable electronic means)

Date: 07/09/2021

City and state: Wilmington, Delaware



Judge's signature

Magistrate Judge Honorable Sherry R. Fallon

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

IN THE MATTER OF THE SEARCH OF AN
APPLE IPHONE, A PHOTOGRAPH OF
WHICH IS INCLUDED IN ATTACHMENT
A, CURRENTLY LOCATED AT THE FBI
OFFICE AT 500 DELAWARE AVENUE,
SUITE 300, WILMINGTON, DELAWARE
19801

Case No. _____

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH**

I, Joshua Wilson, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been since 2004. I am a law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7) and I am authorized by law to conduct investigations and to make arrests for felony offenses. I have conducted numerous criminal investigations and executed several search warrants, including for electronic devices and email accounts.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. As set forth

herein, the FBI is investigating Delaware State Police (“DSP”) Trooper Jamal Merrell (“Merrell”) for suspected violations of Title 18, United States Code, Section 242 (Deprivation of Civil Rights).¹ Your affiant has probable cause to believe that evidence of this offense is located on the target device described in Attachment A.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is an Apple iPhone with no model number of serial number visible, photographs of which are included in Attachment A. The Device is currently located at the FBI Baltimore Division, Wilmington Resident Agency Office, located at 500 Delaware Avenue, Suite 300, Wilmington, Delaware, 19801.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. On or about July 6, 2021, _____ and his attorney presented themselves at the Baltimore Division of the Federal Bureau of Investigation, Wilmington, Delaware Resident Agency to report suspicious incidents that had occurred during the past several months at _____’s business, _____, located at _____. _____ has been in operation for approximately ten years and is commonly referred to as a re-shipping company. _____ receives packages from individuals and merchants for the purpose of shipping those items overseas. For example, if the

¹ Section 242 prohibits any person from, under color of law, depriving another of any rights, privileges, or immunities secured or protected by the Constitution or laws of the United States.

online merchant Amazon did not ship to a specific country, Amazon could forward a purchase to [redacted] for shipment to that country. [redacted]'s business location consists of warehouse space and an office. The [redacted] location also connects to an unoccupied warehouse bay which [redacted] uses for egress.

7. [redacted] resides primarily in the country of Georgia, but recently travelled to the United States when he learned of suspicious activity. Specifically, employees reported to

[redacted] that DSP Trooper Merrell visited [redacted] on at least ten occasions beginning in or around February 2021. During Merrell's first visit to [redacted], he gathered the [redacted] employees present and informed them he was conducting an investigation. Merrell explained that, pursuant to his investigation, he would need to inspect packages in the warehouse. Merrell insisted he be left alone during these inspections. [redacted] reported Merrell could be observed on surveillance video opening large shipping boxes, removing individual items from within these larger containers, and placing the items in a [redacted] cart. Merrell would then move the cart containing items to an area outside of surveillance video coverage, in the unoccupied warehouse area near an exterior door. Merrell would return an empty cart at the conclusion of these inspections. Merrell was also observed re-taping the larger shipping boxes from which he had removed items. Merrell did not provide any legal process, obtain written consent from employees or [redacted], nor provide a receipt for any property removed from [redacted]. [redacted] reported that he has received in excess of \$20,000 of claims from customers for items missing from shipments or never received by customers since February 2021. This loss amount is significantly higher than any loss amount [redacted] has experienced in previous years.

8. On July 8, 2021, FBI and DSP conducted a non-custodial interview of Merrell at his residence. During this interview, Merrell stated he had been conducting an investigation involving [REDACTED] and had visited the location numerous times. Merrell stated he first became aware of [REDACTED] when he received a complaint regarding missing merchandise that had been shipped to [REDACTED] in June of 2020. Merrell stated the missing merchandise was recovered at [REDACTED] and Merrell submitted it as evidence to DSP. Merrell stated he conducted internet research which revealed numerous complaints regarding fraudulent purchases, for example stolen goods, shipped to [REDACTED].

9. Subsequently, Merrell conducted regular visits to [REDACTED] while on duty and in uniform where he stated he received verbal consent from employees to conduct searches for suspicious packages. Merrell stated he collected numerous items from the [REDACTED] location that he deemed suspicious. Merrell's criteria for deeming a package suspicious was exterior damage to the packaging of items. Merrell did not provide a receipt for the items he seized and did not report these seizures to his superiors. Merrell stated he maintained possession of these items in his DSP vehicle and would occasionally bring them into his home out of concern of a theft from the vehicle. Merrell stated he conducted internet research on the status of these items during his personal time to attempt to determine if these items were obtained fraudulently. Merrell was unable to determine if any of the items he seized were connected to fraudulent activity.

10. After becoming aware of a possible complaint lodged by [REDACTED] Merrell brought several items to DSP Troop 2 and placed them in the building's sally port (not the designated evidence locker) and left an inventory of the items he seized over the course of the preceding months. These items consisted of several electronic devices, such as computer laptops and cellular phones, and other merchandise in their original packaging.

11. During the interview, Merrell was asked if he sold any items he obtained from . In response, Merrell stated that he had been informed by an employee of that a specific location within was designated as “trash” and contained items that had been damaged in transit or had gone unclaimed for a significant period of time and would be disposed of eventually. Merrell estimated that he had collected and sold approximately 100 iPhones from this “trash” designated area. He sold the iPhones on three separate occasions to an individual who was advertising on the social media platform Facebook as a purchaser of iPhones. He described this individual as an unknown Hispanic male and provided the individual’s phone number to investigators by accessing his cellular phone in the presence of investigators. Merrell received payment for these iPhones in the form of cash or via the online financial application CashApp. Merrell again accessed his cellular telephone in the presence of investigators to provide his CashApp account identifier as “\$Jammerrell”. Merrell also stated he communicated with at least one employee via his cellular telephone and provided the employee’s phone number to law enforcement officers by referencing his cellular phone.

12. At the conclusion of the interview with Merrell, investigators asked Merrell if he would consent to the seizure and search of his cellular telephone. Merrell said he wanted to consider whether to consent to a search for a couple of days and wanted to maintain possession of his cellular telephone during that time. Fearing that Merrell would delete evidence from his cellular telephone, Special Agent Wilson and another FBI agent seized the device with intent to file the instant application for a warrant to search the device.

13. The Device is currently in storage at the FBI Baltimore Division, Wilmington Resident Agency Office, located at 500 Delaware Avenue, Suite 300, Wilmington, Delaware,

19801. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the FBI.

TECHNICAL TERMS

14. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

e. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

15. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

16. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

17. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to coordinate a time and place to engage in criminal conduct or receive payment for criminal conduct, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense. In particular, based on the facts set forth herein, I believe that the device described in

Attachment A may contain evidence of discussions with an employee of TTL regarding seizing merchandise from TTL and/or coordination with other individuals to sell improperly seized items, including records of communications, GPS data from meetings, photographs of items advertised, and/or payments received for improperly seized merchandise.

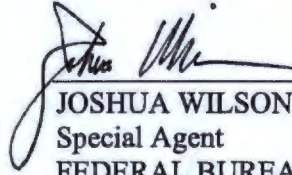
18. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

19. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

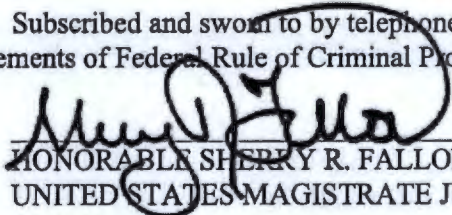
20. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



JOSHUA WILSON
Special Agent
FEDERAL BUREAU OF INVESTIGATION

Subscribed and sworn to by telephone, a reliable electronic means in accordance with the requirements of Federal Rule of Criminal Procedure 4.1, by me, on July 9, 2021:



HONORABLE SHERRY R. FALLON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is an Apple iPhone with no model number of serial number visible, photographs of which are included below. The Device is currently located at the FBI Baltimore Division, Wilmington Resident Agency Office, located at 500 Delaware Avenue, Suite 300, Wilmington, Delaware, 19801.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.



ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 18, United States Code, Section 242 by Merrell since June 1, 2020, including:

- a. lists of merchandise and items seized and related identifying information;
- b. identifying information for individuals Merrell may have conducted transactions with relating to items seized.
- c. types, amounts, and prices of merchandise sold as well as dates, places, and amounts of specific transactions, including methods of payment;
- d. any information recording Merrell's schedule or travel from June 1, 2020 to the present;
- e. All communications between Merrell and individuals associated with or purchasers of items seized.
- f. all bank records, checks, credit card bills, account information, and other financial records including through cash applications;
- g. photographs and screenshots

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Evidence of usage of the internet to facilitate transactions, including:

- a. records of Internet Protocol addresses used;
- b. records of Internet activity, including applications (apps), firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.